UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/712,505 | 11/14/2000 | Kevin R. Driscoll | H16-26353 | 9114 |

128 7590 12/01/2006

HONEYWELL INTERNATIONAL INC.
101 COLUMBIA ROAD
P O BOX 2245
MORRISTOWN, NJ 07962-2245

| EXAMINER | |
|---|---|
| JACKSON, JENISE E | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

DATE MAILED: 12/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/712,505 | DRISCOLL, KEVIN R. | |
| | Examiner | Art Unit | |
| | Jenise E. Jackson | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *05 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 7-13, 16-22, 24, 26-35, 37, 39-43* is/are rejected.

7)☒ Claim(s) *5,6,14,15,23,25,36 and 38* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

2. Claims 1-4, 7-13, 16-22, 24, 26-35, 37, 39-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Coppersmith et al(6,185,679).

3. As per claims 1, 9-11, 18, Coppersmith et al. discloses a source for providing an encryption keystream(see col. 10, lines 33-67)an encryption combiner receiving a first plaintext binary data sequence(see col. 11, lines 45-55) and the encryption keystream and performing a first set of two non-associative operations on the first plaintext binary data sequence(see col. 16, lines 7-41) and the encryption keystream to provide a ciphertext binary data sequence(see col. 7, lines 7-41); a source for providing a decryption keystream; and a decryption combiner receiving the ciphertext binary data sequence and the decryption keystream(see fig. 3, sheet 3) and performing a second set of two non-associative operations on the ciphertext binary data sequence and the decryption keystream to provide a second plaintext binary data sequence that is the same as the first plaintext binary data sequence(see col. 18, lines 65-67, col. 19, lines 1-22).

4. As per claim 2, Coppersmith discloses the stream cipher cryptosystem wherein each operation in the second set is the inverse of an operation in the first set( col. 18, lines 65-67, 65-67, col. 20, lines 1-20).

5. As per claim 3, Coppersmith discloses the stream cipher cryptosystem wherein the operations in the first set include an integer addition operation and an XOR operation, and the operations in the second set include an integer subtraction operation and an XOR operation(see col. 16, lines 7-41, col. 18, lines 65-67, col. 19, lines 65-67, col. 20, lines 1-20, figure 3, sheet 3).

6. As per claim 4, Coppersmith discloses the stream cipher cryptosystem wherein the operations in the first set include an integer subtraction operation and an XOR operation, and the operations in the second set include an integer addition operation and an XOR operation(see col. 16, lines 7-41, col. 18, lines 65-67).

7. As per claim 7, Coppersmith discloses the stream cipher cryptosystem, wherein the operations in the first set include a rotate right operation and an XOR operation, and the operations in the second set include a, rotate left operation and an XOR operation(see fig. 6A and 6B, sheet 6 and 8, col. 17, lines 1-67, col. 18, lines 12-49).

8. As per claim 8, Coppersmith discloses the stream cipher cryptosystem wherein the operations in the first set include a rotate left operation and an XOR operation, and the operations in the second set include a rotate right operation and an XOR operation(see fig. 6A and 6B, sheet 6 and 8, col. 17, lines 1-67, col. 18, lines 12-49).

9. As per claim 12, Coppersmith discloses stream cipher cryptosystem wherein the two sequential non-associative operations are an integer addition operation and an XOR operation(col. 16, lines 7-41, col. 18, lines 65-67, col. 19, lines 65-67, col. 20, lines 1-20, figure 3, sheet 3).

10. As per claim 13, Coppersmith discloses the stream cipher cryptosystem wherein the two sequential non-associative operations are an integer subtraction operation and an XOR operation (see col. 16, lines 7-41, col. 18, lines 65-67).

11. As per claim 16, Coppersmith discloses the stream cipher cryptosystem of wherein the two sequential non-associative operations are a rotate; right operation and an XOR operation(see fig. 6A and 6B, sheet 6 and 8, col. 10, lines 15-16, col. 17, lines 1-67, col. 18, lines 12-49).

12. As per claims 17, 29, Coppersmith discloses the stream cipher cryptosystem of wherein the two sequential non-associative operations are a rotate left operation and an XOR operation(see fig. 6A and 6B, sheet 6 and 8, col. 17, lines 1-67, col. 18, lines 12-49).

13. As per claims 19, 32, Coppersmith discloses wherein the two non-associative operations include an integer addition operation(see col. 16, lines 7-41, col. 18, lines 65-67, figure 3, sheet 3).

14. As per claim 20, Coppersmith discloses the wherein the two non-associative operations include an XOR operation(see col. 16, lines 7-41, col. 18, lines 65-67, col. 19, lines 65-67, col. 20, lines 1-20, figure 3, sheet 3).

15. As per claim 21, Coppersmith discloses wherein the two non-associative operations include an integer subtraction operation(see col. 16, lines 7-41, col. 18, lines 65-67).

16. As per claims 22, 24, 26, Coppersmith discloses wherein the two non-associative operations include an XOR operation(see col. 16, lines 7-41, col. 18, lines 65-67, figure 3, sheet 3).

17. As per claim 27, Coppersmith discloses wherein the two non-associative operations include a rotate right operation(see col. 10, lines 15-16).

18. As per claims 28, 30, limitations already addressed(see claim 24).

19. As per claim 31, limitations have already been addressed(see claim 1).

20. As per claim 32, wherein the two non-associative operations include an integer addition operation(see col. 8, lines 30-65).

21. As per claim 33, already rejected(see claim 24).

22. As per claim 34, already rejected(see claim 21).

23. As per claims 35, 37, 39, limitations already rejected(see claim 24).

24. As per claims 39, 43, limitations already rejected(see claim 24).

25. As per claim 40, limitations already rejected(see claim 27).

26. As per claims 41, 43, limitations already rejected(see claim 24).

27. As per claim 42, limitations already rejected(see claim 7).

28. As per claims 5-6, 14-15, 23, 25, 36 and 38 are objected to as being rejected on base claims. Reasons why these claims are allowable are for the features of inverse modular multiplication and modular multiplication being applied to the same keystream, along with XOR. In symmetric encryption there is no disclosure of using both modular multiplication in combination with another operation.

**Final Action**

**29. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

**Response to Applicant**

30. The 112 second rejection has been withdrawn by the Examiner. The Applicant has amended claim 1 to overcome 112 2nd rejection.

31. The Applicant states that Coopersmith discloses a symmetric block cipher cryptosystems, and the claimed invention calls for a stream cipher cryptosystems.

32. Applicant's arguments filed 9/5/06 have been fully considered but they are not persuasive.

33. In response to applicant's arguments, the recitation "Stream Cipher Cryptosystem" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jenise Jackson

November 26, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100